

# Entanglement verification using local unitary stabilizers

David W. Lyons\* and Scott N. Walck†  
Lebanon Valley College, Annville, PA 17003

(Dated: 25 March 2013)

Local unitary stabilizer subgroups constitute powerful invariants for distinguishing various types of multipartite entanglement. In this paper, we show how stabilizers can be used as a basis for entanglement verification protocols on distributed quantum networks using minimal resources. As an example, we develop and analyze the performance of a protocol to verify membership in the space of Werner states, that is, multi-qubit states that are invariant under the action of any 1-qubit unitary applied to all the qubits.

PACS numbers: 03.67.Mn

## I. INTRODUCTION

Entangled multipartite quantum states of two-level quantum systems, or qubits, play a key role as resources used in quantum computation and quantum communication protocols (see, for example, [1, 2], or [3, 4] for more extensive surveys). In this paper, we consider a basic practical problem in distributed quantum computing: a collection of  $n$  parties will perform a distributed quantum computational task that requires as a resource a particular entangled state, or more generally, any state from a given family of entangled states. An untrusted source provides the resource states, and the parties wish to verify that a resource state is genuine. To minimize the cost of verification, the parties have access to only a limited collection of single-qubit operations. For a survey of entanglement verification protocols, see [5], and for recent work related to this paper, see [6] and its references.

Inspired by [6], in which Pappa et al. treat the verification test problem for the  $n$ -particle GHZ state, we present here a general framework for a verification test protocol for certain types of families of states, namely, families characterized by stabilizing subgroups of the local unitary group. This is motivated by the authors' previous work [7–10] that demonstrates a precise connection between many well-known entanglement resources, such as the GHZ states, Werner states, and permutationally invariant states that include the W states and Dicke states, and their stabilizer subgroups of the local unitary group.

To illustrate the subgroup-based verification protocol general framework, we give a specific test for verification of the family of Werner states, which are those states stabilized by the subgroup of local unitary operators that consist of the same 1-qubit unitary acting on all  $n$  qubits.

The paper is organized as follows. We begin in Section II with the relationship between states and subgroups of the local unitary group. Section III gives the general framework for entanglement verification tests that exploit the connection of states with subgroups. Then in Section IV we give an example of how the general test framework can be used in the case of the family of Werner states.

## II. THE LOCAL UNITARY STABILIZER AS ENTANGLEMENT INVARIANT

Given a pure state  $|\psi\rangle$  or a mixed state  $\rho$  of  $n$ -qubits, the stabilizer subgroup of the local unitary group is defined by

$$\begin{aligned}\text{Stab}_\psi &= \{g \in G: g|\psi\rangle = |\psi\rangle\} \\ \text{Stab}_\rho &= \{g \in G: g\rho g^\dagger = \rho\}\end{aligned}$$

where  $G$  denotes the local unitary group, which can be taken to be  $G = U(1) \times SU(2)^n$  in the case of pure states, or more simply  $G = SU(2)^n$  for mixed states. Two basic facts that make stabilizer groups useful in the study of entanglement are

1. If two states are LU-equivalent, then their stabilizers are isomorphic.
2. Many classes of known useful entanglement resources are characterized by their stabilizer group.

A consequence of the first statement is that the isomorphism class (more precisely, the conjugacy class) of a stabilizer subgroup is an LU-invariant of the corresponding state [11]. The second statement summarizes a program carried out in a series of papers for pure and mixed Werner states and permutationally invariant states [7–10].

The basic idea used in the verification test framework in the next section is the following. We wish to verify whether a given state  $|\Psi\rangle$  is a member of a family  $V$  of entanglement resource states that are stabilized by all local unitary operations in a subgroup  $S$  of the local unitary group. We have at our disposal a measurement  $M$  and a function  $F$  so that  $F \circ M$  is constant on  $V$ . It may be that there are counterfeit states, that is, states not in  $V$ , which nonetheless pass our measurement test by yielding the same result as  $F \circ M$  applied to elements of  $V$ . Here's where the stabilizing group  $S$  comes in. If  $|\Psi\rangle$  is not a genuine member of  $V$ , there are local unitary operations in  $S$  that take  $|\Psi\rangle$  to a new state  $|\Psi'\rangle \neq |\Psi\rangle$ . Our strategy is to carefully choose a small subset of elements of  $T \subset S$  and the function  $F$  so that by randomly applying elements of  $T$ , we guarantee a nonzero probability that the composition  $F \circ M$  applied to  $|\Psi'\rangle$  yields a result different from the value of  $F \circ M$  on  $V$ , and thus will detect counterfeit states.

\*Electronic address: lyons@lvc.edu

†Electronic address: walck@lvc.edu

### III. ENTANGLEMENT VERIFICATION USING LOCAL UNITARY STABILIZERS

Given a subgroup  $S$  of the local unitary group, let  $V(S)$  denote the space of states fixed by every element of  $S$ , that is,

$$V(S) = \{|\psi\rangle : g|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}.$$

**The verification task.** An untrusted source produces  $n$ -qubit pure states that are claimed to be members of a subspace  $V = V(S)$  for some subgroup  $S$  of the local unitary group. The source distributes the qubits of each state it produces, one qubit to each of  $n$  parties. One party, the verifier, seeks to determine whether the states being produced are members of  $V$ . Each of the parties possesses a trusted 1-qubit measurement device that measures in the standard basis, and has the ability to apply any of a finite collection of 1-qubit gates to their own qubit. Each party shares a trusted classical communication channel with the verifier.

**Set-up for the verification test.** The verifier chooses a probability distribution  $p_1, p_2, \dots, p_k$  and elements  $g_1, g_2, \dots, g_k$  in  $S$  and a function  $F$  that takes as inputs Boolean strings of length  $n$  (these come from measuring states in the standard computational basis) and produces integer or Boolean outputs.  $F$  is required to be well-defined on  $V$  in the sense that if we measure a state  $|\psi\rangle \in V$  in the standard basis, then apply  $F$  to the result, then we must get the same output (which, without loss of generality, we may take to be zero), no matter what post-measurement state was obtained.

The verifier chooses elements  $g_i$  and the function  $F$ . Let  $V_0$  denote the space of states  $|\psi\rangle$  for which  $F(x) = 0$  for every possible value  $x$  obtained from measuring  $|\psi\rangle$  in the standard basis. The verifier desires the following two properties.

- (i)  $F(x) = 0$  for every  $x$  obtained by measuring states in  $V$  (in other words,  $V \subseteq V_0$ ), and
- (ii) for every  $|\psi\rangle$  in  $V_0 \setminus V$ , there is a  $g_i$  such that  $g_i|\psi\rangle$  is *not* in  $V_0$ .

Whether both of these properties are possible to achieve will depend upon the local unitary subgroup in question.

Each  $g_i$  is of the form  $g_i = U_1^i \otimes U_2^i \otimes \dots \otimes U_n^i$  for some  $U_j^i$  in  $U(2)$ . Each party  $j$  is provided with the ability to execute the 1-qubit gates  $U_j^1, U_j^2, \dots, U_j^k$ .

**Protocol for the verification test.** Given a state  $|\Psi\rangle$  produced by the source, with qubits distributed to the  $n$  parties, the verifier randomly selects one of the  $g_i$  with probability  $p_i$ . The verifier instructs each party  $j$  to apply  $U_j^i$  to their qubit, so that the state is now  $g_i|\Psi\rangle$ . Then each party measures their qubit in the computational basis and reports the result to the verifier. The verifier applies  $F$  to the binary string  $x$  resulting from the measurements. The verifier accepts  $|\Psi\rangle$  if  $F(x) = 0$ , and rejects otherwise.

It is clear that the protocol accepts states in  $V$  with probability 1. It is less obvious but intuitively plausible that the protocol accepts a counterfeit state  $|\Psi\rangle \notin V$  with

probability bounded below 1. Here is the heuristic argument. If  $|\Psi\rangle \notin V$ , there is some  $g_i$  such that  $g_i|\Psi\rangle \notin V_0$ . There is a nonzero probability  $p_i$  that the verifier chooses  $g_i$  in the first step of the protocol. In this case, when we now measure  $g_i|\Psi\rangle$  and apply  $F$ , we are *not guaranteed* to get 0, and it seems likely that there should be a way to engineer the  $g_i$ s so that there is a guaranteed nonzero probability that we get an  $F$  value other than zero. The difficult part of proving the effectiveness of a protocol is showing that the collection of  $g_i$ s and the function  $F$  do indeed guarantee a nonzero probability of rejecting  $|\Psi\rangle \notin V$ . In the next section, we give the details and prove that the protocol works for a test to verify membership in the Werner subspace.

### IV. EXAMPLE: TEST FOR PURE WERNER SUBSPACE MEMBERSHIP

The space  $\mathcal{W}$  of  $n$ -qubit pure Werner states is defined to be those states  $|\psi\rangle$  that satisfy

$$U^{\otimes n}|\psi\rangle = |\psi\rangle$$

(up to phase) for all  $2 \times 2$  unitaries  $U$ . The space  $\mathcal{W}$  is sometimes called the *decoherence free subspace for collective decoherence*. It is known [12] that there are no pure Werner states for odd  $n$  qubits, and the space of pure Werner states for even  $n$  qubits is spanned by the set of products of singlet states  $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$  in various pairs of qubits.

**Set-up for the Werner verification test.** An untrusted source produces an  $n = 2m$  qubit state  $|\Psi\rangle$ , and distributes the qubits, one to each of  $n$  parties. The verifier, say, Party 1, chooses probability distribution  $p_0 = p_1 = 1/2$  and local unitaries  $g_0 = \text{Id}, g_1 = H^{\otimes n}$ , where  $H$  is the Hadamard matrix. Let  $F$  be the function that returns the number of 1's minus the number of 0's in a  $n$ -bit Boolean string. Observe that the value of  $F$  is zero on all strings  $x$  that result from measuring a Werner state in the standard basis.

**Werner verification protocol.** The verifier selects either  $g_0, g_1$  with equal probability, and instructs all parties to apply a Hadamard gate to their qubit if  $g_1$  is selected. Each party  $j$  reports measurement result  $x_j$ . The verifier evaluates  $F(x) = F(x_1 x_2 \dots x_n)$  and accepts  $|\Psi\rangle$  if the result is 0, and rejects otherwise.

Because any Werner state  $|\Psi\rangle$  is a superposition of singlet products, the protocol clearly accepts  $|\Psi\rangle$  when  $g_0$  is selected. Because  $H^{\otimes n}|\Psi\rangle = |\Psi\rangle$  and  $H$  takes the  $|0\rangle, |1\rangle$  basis to the  $|+\rangle, |-\rangle$  basis, the protocol accepts  $|\Psi\rangle$  when  $g_1$  is selected. The following theorem shows that the probability of false acceptance of a counterfeit state is bounded by a probability less than 1.

**Theorem 1.** Suppose that  $\langle \Psi | P_{\mathcal{W}} | \Psi \rangle = 1 - \epsilon^2$ , where  $P_{\mathcal{W}}$  is projection onto the Werner subspace. Then we have

$$\Pr(\text{accept } \Psi) \leq 1 - \frac{\epsilon^2}{2}(1 - m)$$

where  $m < 1$  is the maximum fidelity  $\max\{|\langle u|v\rangle|\}$  between normalized states  $|u\rangle, |v\rangle$  that lie in subspaces to be described below.

**Comments.** We point out that our protocol recovers Theorem 1 of [6] for  $n = 2$ . In that case, the Werner subspace is the 1-dimensional span of the singlet, which is local unitary equivalent to  $|\Phi_0^2\rangle$  in [6]. The maximum inner product  $m$  in our Theorem 1 is 0, so the probability of acceptance is the same as in [6].

**Proof of Theorem 1.** It is convenient to give names to a number of subspaces of the Hilbert space  $\mathcal{H}$  of pure states of  $n = 2k$  qubits. As we have already noted, let  $\mathcal{W}$  denote the Werner subspace. Let  $S$  be the span of the weight  $k$  standard basis vectors, and let  $T$  be the span of the weight  $k$   $+$ ,  $-$  basis vectors. A key fact that makes Theorem 1 possible is that  $\mathcal{W} = S \cap T$  (see Lemma 1 in the Appendix). Let  $U = \mathcal{W}^\perp \cap S$  and let  $V = \mathcal{W}^\perp \cap T$ . Let  $S' = S^\perp \cap (S + T)$  and let  $T' = T^\perp \cap (S + T)$ . Finally, let  $L = (S + T)^\perp$ . For each of these spaces  $A$ , let  $P_A$  denote the projection onto  $A$ . Let  $m$  denote the maximum inner product between unit vectors in  $U, V$ , that is,

$$m = \max\{|\langle\psi|\phi\rangle| : |\psi\rangle \in U, |\phi\rangle \in V, \langle\psi|\psi\rangle = \langle\phi|\phi\rangle = 1\}.$$

We can write any  $|\Psi\rangle$  in  $\mathcal{H}$  as an orthogonal sum

$$|\Psi\rangle = P_{\mathcal{W}}|\Psi\rangle + P_{U+V}|\Psi\rangle + P_L|\Psi\rangle.$$

We further decompose  $P_{U+V}|\Psi\rangle$  in two different orthogonal sums.

$$P_{U+V}|\Psi\rangle = P_U|\Psi\rangle + P_{S'}|\Psi\rangle \quad (1)$$

$$P_{U+V}|\Psi\rangle = P_V|\Psi\rangle + P_{T'}|\Psi\rangle \quad (2)$$

Given that the trace distance from  $|\Psi\rangle$  to the nearest pure Werner state vector is  $\epsilon$ , that is,  $\langle\Psi|P_{\mathcal{W}}|\Psi\rangle = 1 - \epsilon^2$ , we can define  $\epsilon_1, \epsilon_2, \alpha, \beta$  (positive quantities that sum to  $\epsilon^2$ )

as follows.

$$\langle\Psi|P_{U+V}|\Psi\rangle = \epsilon_1^2 \quad (3)$$

$$\langle\Psi|P_L|\Psi\rangle = \epsilon_2^2 \quad (4)$$

$$\langle\Psi|P_U|\Psi\rangle = \alpha^2 \quad (5)$$

$$\langle\Psi|P_V|\Psi\rangle = \beta^2 \quad (6)$$

The probability of acceptance of  $|\Psi\rangle$  by our protocol is given by

$$\begin{aligned} \Pr(\text{accept } \Psi) &= \frac{1}{2}\langle\Psi|P_S|\Psi\rangle + \frac{1}{2}\langle\Psi|P_T|\Psi\rangle \\ &= 1 - \epsilon^2 + \frac{\alpha^2 + \beta^2}{2}. \end{aligned}$$

Applying Lemma 2 in the Appendix to the unit vector  $\frac{P_{U+V}|\Psi\rangle}{\langle\Psi|P_{U+V}|\Psi\rangle}$ , we have  $\alpha^2 + \beta^2 \leq (1 + m)\epsilon_1^2$ , which is in turn less than or equal to  $(1 + m)\epsilon^2$ . The conclusion of the Theorem follows.

## V. OUTLOOK

We know that  $m = 0$  for  $n = 2$ , and have numerically calculated that  $m = 1/2$  for  $n = 4, 6, 8, 10$ . We conjecture that  $m = 1/2$  for  $n = 2k$  with  $k \geq 2$ . It will be interesting to apply the general stabilizer framework to further classes of states.

**Acknowledgments.** The authors thank Elena Diamanti and Damian Markham for helpful conversations, and also Philip Spain for pointing out a useful reference for the proof of Lemma 2.

- 
- [1] Charles H. Bennett, Gilles Brassard, Claude Crpeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895 – 1899, 1993.
  - [2] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*. IEEE Press, Los Alamitos, CA, 1994.
  - [3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
  - [4] Stan Gudder. Quantum computation. *American Mathematical Monthly*, 110:181, 2003.
  - [5] S. J. van Enk, N. Lütkenhaus, and H. J. Kimble. Experimental procedures for entanglement verification. *Phys. Rev. A*, 75:052318, May 2007.
  - [6] Anna Pappa, André Chailloux, Stephanie Wehner, Eleni Diamanti, and Iordanis Kerenidis. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.*, 108:260502, Jun 2012. arXiv:1112.5064.
  - [7] David W. Lyons, Scott N. Walck, and Stephanie A. Blanda. Classification of nonproduct states with maximum stabilizer dimension. *Phys. Rev. A*, 77:022309, 2008. arXiv:0709.1105 [quant-ph].
  - [8] Curt D. Cenci, David W. Lyons, and Scott N. Walck. Local unitary group stabilizers and entanglement for multi-qubit symmetric states. *Accepted, Springer Lecture Notes in Computer Science*, 2011. arXiv:1011.5229v1 [quant-ph].
  - [9] David W. Lyons and Scott N. Walck. Symmetric mixed states of  $n$  qubits: Local unitary stabilizers and entanglement classes. *Phys. Rev. A*, 84:042340, October 2011. arXiv:1107.1372v1 [quant-ph].
  - [10] David W. Lyons, Abigail M. Skelton, and Scott N. Walck. Werner state structure and entanglement classification. *Advances in Mathematical Physics*, 2012:463610, 2012. arXiv:1109.6063v2 [quant-ph].
  - [11] Curt D. Cenci, David W. Lyons, Laura M. Snyder, and Scott N. Walck. Symmetric states: local unitary equivalence via stabilizers. *Quantum Information and Computation*, 10:1029–1041, November 2010. arXiv:1007.3920v1 [quant-ph].
  - [12] David W. Lyons and Scott N. Walck. Multiparty quantum states stabilized by the diagonal subgroup of the local unitary group. *Phys. Rev. A*, 78:042314, October 2008. arXiv:0808.2989v2 [quant-ph].
  - [13] Jr. R. P. Boas. A general moment problem. *American Journal of Mathematics*, 63(2):361–370, April 1941. <http://www.jstor.org/stable/2371530>.

## VI. APPENDIX

**Lemma 1.** The Werner subspace  $\mathcal{W}$  of  $n = 2k$  qubit pure states, that is,

$$\mathcal{W} = \{|\psi\rangle : U^{\otimes n} |\psi\rangle = |\psi\rangle \text{ for all } U \in U(2)\},$$

is the intersection  $S \cap T$  of the subspaces

$S$  = span of the weight  $k$  basis vectors in the  $0, 1$  basis  
 $T$  = span of the weight  $k$  basis vectors in the  $+, -$  basis.

**Proof.** We show in [12] that any pure Werner state is a superposition of products of the singlet state  $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ , so it is clear that  $\mathcal{W} \subset S$ . The Hadamard matrix  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  takes  $|0\rangle, |1\rangle$  to  $|+\rangle, |-\rangle$ , so  $H^{\otimes n}$  takes  $S$  to  $T$ . Since  $H^{\otimes n}$  fixes every state in  $\mathcal{W}$ , we have  $\mathcal{W} \subset T$ . Conversely, suppose we have a state  $|\psi\rangle$  in  $S \cap T$ . Because  $|\psi\rangle \in S$ , it is a simple calculation that

$$\left. \frac{d}{dt} \right|_{t=0} (\exp(itZ) \otimes \cdots \otimes \exp(itZ)) |\psi\rangle = 0$$

where  $Z$  is the Pauli  $Z$  matrix (see, for example, [7]). Likewise, because  $|\psi\rangle \in T$ , we have

$$\left. \frac{d}{dt} \right|_{t=0} (\exp(itX) \otimes \cdots \otimes \exp(itX)) |\psi\rangle = 0$$

where  $X$  is the Pauli  $X$  matrix. Because  $(iZ, iZ, \dots, iZ), (iX, iX, \dots, iX)$  generate the Lie algebra of the subgroup  $\Delta = \{(U, U, \dots, U) : U \in SU(2)\}$  that defines the Werner subspace, we conclude that  $|\psi\rangle$  is in  $\mathcal{W}$ .

**Lemma 2.** Let  $U, V$  be subspaces of a Hilbert space  $H$  of any dimension, and let  $P_U, P_V$  be the orthogonal

projections onto  $U, V$ , respectively. Let  $|\Psi\rangle$  be a unit vector  $H$ , and let

$$m = \max\{|\langle\psi|\phi\rangle| : |\psi\rangle \in U, |\phi\rangle \in V\}, \langle\psi|\psi\rangle = \langle\phi|\phi\rangle = 1\}.$$

Then

$$\langle\Psi|P_U|\Psi\rangle + \langle\Psi|P_V|\Psi\rangle \leq m + 1.$$

**Proof.** Let  $|\Psi\rangle$  be given. Define unit vectors  $|u\rangle \in U, |v\rangle \in V$  by

$$|u\rangle = \frac{P_U |\Psi\rangle}{\sqrt{\langle\Psi|P_U|\Psi\rangle}}$$

$$|v\rangle = \frac{P_V |\Psi\rangle}{\sqrt{\langle\Psi|P_V|\Psi\rangle}}$$

(if  $P_U |\Psi\rangle = 0$ , choose any unit vector in  $U$  for  $|u\rangle$ , and similarly for  $|v\rangle$  in the case that  $P_V |\Psi\rangle = 0$ ) so that we have

$$\langle\Psi|P_U|\Psi\rangle = |\langle\Psi|u\rangle|^2$$

$$\langle\Psi|P_V|\Psi\rangle = |\langle\Psi|v\rangle|^2.$$

A generalization of Bessel's inequality [13] says that

$$|\langle\Psi|u\rangle|^2 + |\langle\Psi|v\rangle|^2 \leq 1 + |\langle u|v\rangle|$$

so we have

$$\begin{aligned} & \langle\Psi|P_U|\Psi\rangle + \langle\Psi|P_V|\Psi\rangle \\ &= |\langle\Psi|u\rangle|^2 + |\langle\Psi|v\rangle|^2 \\ &\leq 1 + |\langle u|v\rangle| \\ &\leq 1 + m. \end{aligned}$$